UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

AMERICAN GUARD SERVICES, INC., a California corporation,	CASE NO. C18-0603-JCC
Plaintiff,	ORDER
v.	
TERMINAL SERCURITY SOLUTIONS, INC., a California corporation; TOR WALLEN; WAYNE PACK and KAYSSE MOYNIHAN,	
Defendants.	

This matter comes before the Court on the parties' stipulated motion for an order regarding the discovery of electronically stored information ("ESI") and hard copy documents (Dkt. No. 28). Pursuant to the parties' stipulation, the Court ORDERS the following:

I. SCOPE

This Agreement shall govern how the parties manage electronic discovery in the above captioned case and all actions that are later consolidated with that case (collectively, the "Litigation"). The parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith throughout the Litigation. The proportionality standard set forth in

Federal Rule of Civil Procedure 26(b)(2)(C) shall be applied in the Litigation when formulating the discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses for the Litigation should be reasonably targeted, clear, and as specific as possible. Nothing in this Agreement shall be interpreted as requiring a party to re-produce documents per the terms of this Agreement, where those documents were disclosed prior to the mutual execution and effective date of this Agreement, absent a showing of good cause.

II.   eDISCOVERY LIAISONS

The parties have identified liaisons to each other who are and will be knowledgeable about and responsible for discussing their respective ESI ("eDiscovery Liaisons"). Each eDiscovery Liaison will be, or have access to those who are, knowledgeable about the technical aspects of eDiscovery, including the location, nature, accessibility, format, collection, search methodologies, and production of ESI in the Litigation. The parties will rely on the eDiscovery Liaisons, as needed, to confer about ESI and to help resolve disputes without court intervention. The eDiscovery Liaisons for each of the parties are as follows:

Delaney Waldron KLINEDINST PC Dwaldron@klinedinstlaw.com (619) 239-8131	eDiscovery Liaison for Plaintiff AMERICAN GUARD SERVICES, INC.
Ross Merritt JACKSON LEWIS P.C. Ross.merritt@jacksonlewis.com (206) 626-6408	eDiscovery Liaison for Plaintiff AMERICAN GUARD SERVICES, INC.
Joshua Tolles DAVIS WRIGHT TREMAINE LLP joshuatolles@dwt.com (206) 757-8368	eDiscovery Liaison for Defendants TERMINAL SECURITY SOLUTIONS, INC.; TOR WALLEN; and WAYNE PACK

If the parties need to modify their designated eDiscovery Liaisons, the party effecting the changes shall notify all other parties within five (5) business days of the change, including the new contact information for the eDiscovery Liaison.

III. PRESERVATION

Consistent with the parties' obligations under Federal Rule of Civil Procedure 26(f), the parties have met and conferred regarding the scope of preservation, including custodians, data sources, date ranges, and categories of information that have been or should be preserved in connection with the Litigation. The parties will disclose categories or sources of responsive information that it has reason to believe have not been preserved or should not be preserved, and will explain with specificity the reasons to support such a belief.

The parties acknowledge that they have a common law obligation to take reasonable and proportional steps to preserve discoverable information in their possession, custody, or control. With respect to the preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody, or control.

2. All parties shall supplement their disclosures made in accordance with Federal Rule of Civil Procedure 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made.

3. Absent a showing of good cause by the requesting party, and absent agreement to the contrary evidenced in **Exhibit A** of this Agreement, the following categories of ESI need not be preserved:

a. Deleted, slack, fragmented, or other data only accessible by forensics.

b.   Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

c.   Online access data such as temporary internet files, history, cache, cookies, and the like.

d.   Data in metadata fields that are frequently updated automatically, such as last-opened dates.

e.   Back-up data that are substantially duplicative of data that are more accessible elsewhere.

f.   Server, system, or network logs.

g.   Data remaining from systems no longer in use that is unintelligible on the systems in use (*i.e.*, legacy systems).

IV.   IDENTIFICATION OF RESPONSIVE DOCUMENTS

The parties have met and conferred to discuss how to proceed with discovery in the most efficient and effective manner. The instant Agreement indicates an attempt to, in good faith, come to an agreement on search and culling methods used to identify responsive information. The parties met and conferred on **June 20, 2018** regarding this ESI stipulation, and will meet and confer again on the scope of discovery, including custodians, custodial and non-custodial sources, date ranges, file types, or any additional proposed method to cull documents for review (*i.e.*, search terms, technology-assisted-review, predictive coding). The parties agree that the grounds for any objections should be supported by specific information. The parties will not seek court intervention without first attempting to resolve any disagreements in good faith, based upon all reasonably available information.

A.   Sources

The parties have disclosed and discussed the custodial and non-custodial data sources likely to contain responsive information. The parties have identified and described any relevant electronic systems and storage locations, included in **Exhibit A**. The parties retain the right, upon reviewing the initial production of documents and conducting other investigation and discovery,

to request that files from additional custodial or non-custodial sources be searched, and agree to meet and confer regarding any such request.

B.   Identification of Custodians

The parties have identified all persons whose files are likely to contain hard copy documents and ESI relating to the subject matter of the Litigation, included in **Exhibit A**. This includes a description of each proposed custodian's job title and brief description of such person's responsibilities (including dates of employment by the applicable party). The parties retain the right, upon reviewing the initial production of documents and conducting other investigation and discovery, to request that files from additional custodians be searched, and to meet and confer regarding such request.

C.   Easily Segregable Documents

Documents or categories of documents that are easily identifiable and segregable shall be collected without the use of search terms or other agreed upon advanced search methodology (*e.g.*, analytics, predictive coding, technology-assisted-review). The producing party will indicate which categories of documents will be produced with and without the use of search terms or other advanced search methodology. Where potentially responsive ESI shall be searched through the use of search terms, the parties agree to follow the process identified below and that they shall meet and confer regarding any proposed deviation.

D.   Search Terms and Technology-Assisted-Review

The parties shall cooperate in good faith regarding the disclosure and formulation of appropriate search terms and protocols in advance of any search to cull custodians' ESI. With the

objective of limiting the scope of review and production, and thereby reducing discovery burdens, the parties shall meet and confer in good faith regarding the Hit Count Reports and regarding any disputed search terms. The parties shall resolve their differences on any disputed initial search terms or, if unsuccessful, bring the dispute regarding initial search terms to the Court's attention via the appropriate procedure.

If, after completion of the initial search methodology process outlined directly above, a party determines that any search term or terms should be added to the initial search term list, then the requesting party shall advise the producing party in writing of the proposed additional search term or terms. Within seven (7) days of the request for additional search terms, the producing party shall either agree to use the additional search term or terms or provide a revised Hit Count Report that includes the previously agreed terms and the additional requested search term or terms. The parties shall again meet and confer in good faith regarding the Hit Count Reports for any additional disputed search term or terms. If any search term or terms remain in dispute after such time, the parties may bring the matter to the Court via the appropriate procedure.

Hit Count Report: A Hit Count Report must be provided in Microsoft Excel (or other format as agreed to by both parties). A Hit Count Report must include the following information: (a) overall number of documents being searched, (b) number of documents hit by the search term with separate hits for individual documents hit vs. documents hit including families, and (c) unique documents hit by each search term or string (*i.e.*, documents that would not be included in the search results but for the inclusion of that particular search term).

No party shall use predictive coding or technology-assisted-review for the purpose of culling the documents to be reviewed or produced without first notifying the opposing party and providing ample time to meet and confer in good faith regarding a mutually agreeable protocol for the use of such technologies.

E. Family Relationships

Family relationships shall be maintained for all responsive records, unless a claim of privilege is asserted. Family relationships refer to connected records, such as an email (the "parent") with its corresponding attachments (the "children"). If family relationships are severed due to a claim of privilege, the party asserting privilege shall provide a privilege log that includes: the name of the individual or individuals from whom the allegedly privileged document originated; the name of the individual or individuals to whom the allegedly privileged document was directed; the date the allegedly privileged document was created; the title or subject line of the allegedly privileged document, if not the allegedly privileged content itself; the privilege claimed and its basis in law; and the corresponding Group Identifier to identify the broken familial relationship from the privilege log.

V. PRODUCTION OF HARD COPY DOCUMENTS – FORMAT

Hard copy documents shall be scanned as single-page, Group IV, 300 DPI TIFF images with an .opt image cross-reference file and a delimited database load file (*i.e.*, .dat). The database load file should contain the following fields: "BATES BEG," "BATES END," "PAGES," "VOLUME," "CUSTODIAN," and "OCR" (containing a link to the associated document-level OCR text file). The documents should be logically unitized (*i.e.*, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records) and be produced in the order in which they are kept in the usual course of business. If an original document contains color to understand the meaning or content of the document, the document shall be produced as single-page, **300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image**. Multi-page OCR text for each document should also be provided. The OCR software shall maximize text quality over process speed and shall not

include Bates numbers, unless redactions have been applied. Settings such as "auto-skewing" and "auto-rotation" should be turned on during the OCR process.

VI.   PRODUCTION OF ESI

A.   Format

The parties may produce ESI using one of two agreed upon formats – TIFF production or Native production. To the extent that there are rolling productions in the Litigation, each party shall maintain the production format elected and utilized during their initial production volume made subsequent to the execution and terms of this Agreement, unless otherwise agreed by the parties.

TIFF Production: A party may produce responsive documents as single-page, black and white, TIFF Group IV, 300 DPI TIFF images, with the exception of spreadsheet type files, source code, audio, and video files, which shall be produced in their native format. TIFF productions will show any and all text and images which would be visible to the reader using the native software that created the document. For example, TIFF productions of e-mail messages should include the BCC line. PowerPoint documents shall be processed with hidden slides and all speaker notes unhidden, and shall be processed to show both the slide and the speaker's notes on the TIFF production. If an original document contains color, the document should be produced as **single-page, 300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image**. Parties are under no obligation to enhance an image beyond how it was kept in the usual course of business.

If a TIFF production is produced in its native format, a single-page Bates stamped image slip sheet stating the document has been produced in its native format will also be provided. Each such slip-sheet shall also include applicable confidentiality or other similar branding designations

if required for production per the protective order or another similar order or agreement. Each native format document should be named according to the Bates number it has been assigned, and should be linked directly to its corresponding record in the load file using the FILE_PATH field. File names for native format documents shall also include confidentiality or other similar branding designations (*e.g.*, BATES_00000001_HighlyConfidential) if required for production per the protective order or another similar order or agreement. To the extent that either party believes that specific documents or classes of TIFF productions, not already identified within this Agreement, should be produced in their native format, the parties agree to meet and confer in good faith.

Native Production: A party may produce responsive documents as native files (the file format associated with the original creating application, such as a Word document or Outlook document), with the exception of native files that correspond to produced paginated documents that have been redacted or native files that are containers of files (*e.g.*, Zip file containers). Each native file should be named according to the Bates number it has been assigned, and should be linked directly to its corresponding record in the load file using the FILE_PATH field. File names for native files shall also include confidentiality or other similar branding designations as part of the file name (*e.g.*, BATES_00000001_HighlyConfidential) if required for production per the protective order or another similar order or agreement.

In addition, confidential or privilege coding associated with any responsive documents to be produced shall be provided to the requesting party in the corresponding record in the load file to further ensure that any native files are appropriately identified per the protective order or another similar order or agreement. The coding provided shall be used to appropriately brand any native files that are imaged for evidentiary use at any point during the Litigation, including at deposition and trial. Native files imaged for such use shall be branded with the document's Bates number and

page-level suffix numbering (e.g., BATES_00000001.0001) on each page in the lower right hand corner. Confidential or other similar branding shall be applied in the lower left corner of each page.

B.   De-Duplication

Each party shall remove exact duplicate documents, based on MD5 or SHA-1 hash values, at the family level. Attachments should not be eliminated as duplicates for purposes of production, unless the parent e-mail and all attachments are also duplicates. The parties agree that an email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical. Removal of near-duplicate documents and e-mail thread suppression is not acceptable. De-duplication will be done across the entire collection (global de-duplication) and the ALL CUSTODIANS field will list each custodian, separated by a semi-colon, who was a source of that document, and the ALL SOURCE LOCATIONS field will list each file path, separated by a semi-colon, that was a source of that document. Should the ALL CUSTODIANS or ALL SOURCE LOCATIONS metadata fields produced become outdated due to rolling productions, an overlay file providing all the custodians and file paths for the affected documents will be produced prior to substantial completion of production.

C.   Metadata

All ESI, whether produced via TIFF Production or Native Production, shall be produced with a delimited, database load file that contains the metadata fields listed in **Table 1**, attached hereto, to the extent such metadata exists at the time of document collection. The metadata produced should have the correct encoding to enable preservation of the documents' original language.

D.   Embedded Objects

The parties agree to meet and confer over the inclusion or exclusion of embedded files from production.

E.   Compressed Files Types

Compressed file types (*i.e*., .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

F.   Structured Data

To the extent a response to discovery requires production of electronic information stored in a database, including the production of text messages or similar communications, the parties will meet and confer regarding methods of production. The parties will consider whether all relevant information may be provided by querying the database for discoverable information and generating a report in a reasonably usable and exportable electronic file.

G.   Encryption

To maximize the security of information in transit, any media on which ESI or hard copy documents are produced may be encrypted. In such cases, the producing party shall transmit the encryption key or password to the receiving party, under separate cover, contemporaneously with sending the encrypted media. ESI or hard copy documents not produced on physical media shall be transmitted via sFTP or other file transfer protocol that encrypts documents while in motion and at rest.

H.   Redactions

If documents that the parties have agreed to produce in native format need to be redacted, the parties will meet and confer regarding how to implement redactions while ensuring that proper formatting and usability are maintained.

I.   Documents Protected From Discovery

Pursuant to Federal Rule of Evidence 502(e), the production of a privileged or work-product-protected document, whether inadvertent or otherwise, is not a waiver of privilege or protection from discovery in the Litigation. For example, the mere production of privileged or work-product-protected documents in the Litigation as part of a mass production is not itself a waiver in the Litigation. Communications involving trial counsel that post-date the filing of the complaint need not be placed on a privilege log.

\\\

\\

\\

\\

\\

\\

\\

\\

\\

\\

\\

\\

\\

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD, this 2nd day of October, 2018.

KLINEDINST PC

By: *s/ Gregor A. Hensrude*
By: *s/ Stephanie D. Olson*
Gregor A. Hensrude, WSBA #45918
Stephanie D. Olson, WSBA #50100
701 5th Ave., Ste. 1220
Seattle, WA 98104
(206) 682-7701
Email: ghensrude@klinedinstlaw.com
        solson@klinedinstlaw.com
Attorneys for Plaintiff

DAVIS WRIGHT TREMAINE LLP

By: *s/ Greg Hendershott*
By: *s/ Harry J. F. Korrell*
By: *s/ Matthew R. Jedreski*
Greg Hendershott, WSBA #27838
Harry J. F. Korell, WSBA #23173
Matthew R. Jedreski, WSBA #50542
1201 Third Ave., Ste. 2200
Seattle, WA 98101-3045
(206) 622-3150
Email: greghendershott@dwt.com
        harrykorrell@dwt.com
        mjedreski@dwt.com
Attorneys for Defendants Terminal Security Solutions, Inc., Tor Wallen, Wayne Pack

By: *s/ Daniel P. Crowner*
Daniel P. Crowner, WSBA #37136
Jackson Lewis P.C.
520 Pike Street, Suite 2300
Seattle, WA 98101
(206) 405-0404
Email: daniel.crowner@jacksonlewis.com
Attorneys for Plaintiff-Counterclaim Defendant

DATED this 5th day of October 2018.

John C. Coughenour
UNITED STATES DISTRICT JUDGE

ORDER
C18-0603-JCC
PAGE - 13

TABLE I – ESI Metadata Fields

FIELD NAME	DESCRIPTION
Attachment List	List of attachments
Author	Author of document
Bates Beg	Beginning bates number of document
Bates Beg Attach	Beginning bates number of attachment
Bates End	Ending bates number of document
Bates End Attach	Ending bates number of attachment
Comments	For Microsoft documents (ppt speaker notes, cell comments)
Control Number	Beginning bates number for each record
Custodian	Individual who had custody of the document
Date Created	Date and time document was created (Ex. 01/01/2001 17:00)
Date Last Modified	Date and time the document was last modified (Ex. 01/01/2001 17:00)
Date Received	Date and time email was received (Ex. 01/01/2001 17:00)
Date Sent	Date and time email was sent (Ex. 01/01/2001 17:00)
Document Extension	File extension of document (.msg, .docx, .xlsx, etc.)
Email BCC	Blind-copied recipients of email
Email CC	Copied recipients of email
Email From	Sender of email
Email Subject	Subject line of email
Email To	Recipient of email
Extracted Text	Relative file path of text file
File Name	File name
Group Identifier	Unique number that groups parent email and attachments
Last Saved By	Individual whom last modified the document
MD5 Hash	MD5 Hash Value
FILE_PATH	Relative file path of native file
Virtual Path	Original file path where file was kept (by the custodian)
Pages	Number of pages per document
Parent Document ID	Parent control number or parent bates stamp number (this field should only be populated to children, not to the parent itself)
All Custodians	List of all custodians who had custody of the document, separated by semicolon
All Source Location	List of all source locations the document existed among the various custodians' ESI sources; separated by semicolon

ORDER
C18-0603-JCC
PAGE - 14